gta GEORGIA TECHNOLOGY AUTHORITY	**Georgia Technology Authority**	
Title:	**Enterprise IT Supply Chain Security Controls Policy**	
PSG Number:	**PS-20-001**	
Issue Date:	2/1/2020	**Effective Date:** 4/1/2020
Synopsis:	Enterprise-wide IT supply chain management policy.	

PURPOSE

The purpose of this document is to provide guidance to State agencies on identifying, assessing, selecting and implementing risk management processes and controls throughout the enterprise to manage IT supply chain risk. Threats to the IT supply chain come from a variety of malicious actors: counterfeiters, insiders, foreign intelligence services, terrorists, industrial spies and cyber criminals. Risks include the introduction of malicious hardware and software, theft, tampering, and insecure manufacturing, development and production practices.

SCOPE and AUTHORITY

Information Technology Policies, Standards and Guidelines (PM-04-001)

POLICY

The Georgia Technology Authority (GTA) shall, through the authority granted by state law, develop and maintain policies, standards and guidelines to mitigate IT supply chain risk. The standards shall be based on guidance developed by the National Institute of Standards and Technology (NIST) and published in NIST Special Publication 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations).

All agencies shall follow established State policies and standards to implement mitigation strategies to combat supply chain threats whether presented by the supplier, product or supply chain.

Agencies shall include IT supply chain risk management into their risk management framework and ensure that their service providers are

appropriately managing their supply chain risk.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

SS-20-002 Information Technology Supply Chain Security Controls
PS-08-031 Information Security – Risk Management
SS-08-041 Risk Management Framework

REFERENCES

NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

TERMS AND DEFINITIONS

Supply Chain: Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of information and communications technology (ICT) products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.

Supply Chain Risk: Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems

Supply Chain Risk Management: The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.